CYBER ELECTROMAGENTIC ACTIVITIES WITHIN THE MISSION COMMAND WARFIGHTING FUNCTION: WHY IS IT IMPORTANT AND WHAT IS THE CAPABILITY?

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JAMES D. COONFIELD III, MAJOR, US ARMY
B.S., Wayland Baptist University, Plainview, Texas, 2005

Fort Leavenworth, Kansas
2013-02

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 13-12-2013	**2. REPORT TYPE** Master’s Thesis	**3. DATES COVERED** *(From - To)* FEB 2013 – DEC 2013

4. TITLE AND SUBTITLE Cyber Electromagentic Activities within the Mission Command Warfighting Function: Why is it Important and What is the Capability?	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Major James D. Coonfield III	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR’S ACRONYM(S)** **11. SPONSOR/MONITOR’S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Over the past 20 years, the increased incorporation of cyber capabilities into military command and control functions has necessitated an intensive defensive cyber posture for protection, but little effort was put into offensive cyber capabilities. The recent uses of cyber as a means of achieving national goals has changed not only how cyberspace is viewed by military leaders, but has also changed the potential for offensive cyber as a military weapon. This thesis argues for the placement of cyber electromagnetic activities within the Mission Command warfighting function by identifying the capability that cyber electromagnetic activities provides to military operations.

15. SUBJECT TERMS
Cyber Electromagnetic Activities, CEMA, Mission Command, Cyber

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	62	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major James D. Coonfield III, U.S. Army

Thesis Title: Cyber Electromagnetic Activities within the Mission Command Warfighting Function: Why is it Important and What is the Capability?

Approved by:

____, Thesis Committee Chair
Michael H. McMurphy, M.S.

____, Member
Phillip G. Pattee, Ph.D.

____, Member
John M. Sullivan, M.S.

Accepted this 13th day of December 2013 by:

____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

CYBER ELECTROMAGENTIC ACTIVITIES WITHIN THE MISSION COMMAND WARFIGHTING FUNCTION: WHY IS IT IMPORTANT AND WHAT IS THE CAPABILITY?, by MAJ James D. Coonfield III, 62 pages.

Over the past 20 years, the increased incorporation of cyber capabilities into military command and control functions has necessitated an intensive defensive cyber posture for protection, but little effort was put into offensive cyber capabilities. The recent uses of cyber as a means of achieving national goals has changed not only how cyberspace is viewed by military leaders, but has also changed the potential for offensive cyber as a military weapon. This thesis argues for the placement of cyber electromagnetic activities within the Mission Command warfighting function by identifying the capability that cyber electromagnetic activities provides to military operations.

ACKNOWLEDGMENTS

This thesis would not have been possible without the guidance, opinions, and advice of the instructors of the Command and General Staff College at Fort Leavenworth. I would like to thank my Staff Group Advisor, Mr. Mike McMurphy, for his instruction and insight, both in class and during multiple discussions out of it. His ability as both an instructor and mentor is indicative of the high quality instructors at the Command and General Staff College.

So many other instructors helped, either directly or indirectly, during the formulation of this thesis. I would like to thank Dr. Phillip Pattee, Mr. John Sullivan, Dr. Richard Faulkner, Mr. Scott Martin, and LTC Andrew Murray, as well as individuals from both ARCYBER and the Mission Command Center of Excellence. Their efforts and perceptions proved to be instrumental in the development of this thesis.

I would also like to express my appreciation to Staff Group 3C for providing both guidance and support in completing this thesis. Not only did they support my efforts, but they exhibited a great deal of patience during multiple break-time discussions in which I tested ideas and concepts.

Finally, I would like to thank my wife, Shelton. Without her patience and support, I might never have completed this thesis. I thank her and the other professionals with whom I was gifted to meet for all of their efforts.

TABLE OF CONTENTS

ACRONYMS

ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
CEMA	Cyber-Electromagnetic Activities
DOD	Department of Defense
EMSO	Electronic Spectrum Operations
EW	Electronic Warfare
FM	Field Manual
IED	Improvised Explosive Device
JP	Joint Publication
WFF	Warfighting Function

ILLUSTRATIONS

CHAPTER 1

INTRODUCTION

Cyber: The New Realm for Warfare

Digital information networks have redefined our operating environment, changing not only how we must think, but also how we must operate in a world where anyone can be an enemy, or an enemy can be anywhere. No longer are we, or our enemies, constrained to operational lines, areas of operation, or even to lines of sight in an attempt to control the battlefield. Computers are the new weapons systems and the new targets are the electronic networks controlling communications and energy infrastructure. Attacks can be directed by any country or any group, spurred by political, social, or economic motivation. This new dimension, this thing we term cyberspace, incorporates a new freedom of movement into hostile operations, as well as a new fear for how to defend ourselves. To some, cyber is nothing more than access to the network, something that is "there," existing for our use and an inconvenience when it does not work. To others, cyber is the most important thing in their operations, enabling access to simultaneous points on the battlefield and guiding the course of an ever-changing environment. The question of whether cyber is an important aspect of military operations depends upon what cyber is used for in the operation and depends upon who is using cyber in that operation.

The DOD Dictionary of Military Terms defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[1] Basically put, cyberspace is an electronic environment consisting of devices, networks, and the hardware they connect to. It is not a tangible environment one can see or feel, but one that is capable of operating faster than thought, transferring data around the globe in the blink of an eye.

There are approximately 1.1 billion devices transmitting and receiving data currently connected to this thing we term the cyber domain. These devices increase our productivity and our ability to "connect" socially, but they also increase our risk. Cyber continues to be used as a means to steal proprietary secrets from corporations, state secrets from governments, and even as a means to achieve political goals, all while cloaking the identities of the organization within a web of social anonymity. The ability to target anything connected to the network by an almost anonymous group, to include infrastructure and energy girds, is frightening.

So why is cyber important? Today's operational environment is extremely complex based upon both the threats we face and the technology available to our adversaries. Cyber introduces data as a weapon on the battlefield, electronic pulses sent from one machine to another through the cyber domain. This data, when assembled at the endpoints, creates information. For military organizations, the most reliable data equates to the ability to assemble the most reliable information, increasing the unit's ability to achieve the best situational understanding of events occurring on the battlefield. Adversely, the ability to manipulate that same information, to alter it, can lead to the making of decisions that are unfavorable to the military operation.

This concept of providing reliable data to Army commanders has been the cornerstone of our early network operations, leading to many advances not only in our technology, but also in our user policies. Recent increases in attacks on our networks, however, have highlighted not only the versatility of cyber-attacks to target military and civilian infrastructure, but also the capability of cyber as a weapon with military applications.

A Brief History of Cyber Warfare

Compared to many of the weapons currently in use by the modern military, digital computers and their realm of operation are relatively new inventions, yet it can be argued that nations have been using computers for warfare purposes for over 60 years. It was in 1943 that the British used the first programmable digital machine, Colossus, to decipher vast quantities of encrypted German messages.[2] Although simple in complexity to today's computers, Colossus is still considered the first electronic computer.

In 1968, the Advanced Research Projects Agency Network (ARPANET) became the operational packet-switching network. The network was initially deigned for universities and research laboratories to facilitate information sharing. ARPANET is the same network that would become what we now call the internet, with about 2.6 million users around the globe in 1990.

In 1982, U.S. officials launched Farewell in an attempt to counter Soviet expansionism. Flawed computer chips, purchased by Soviet agents, found their way into Soviet military equipment and chemical plants. Defective plans and information were introduced for a wide array of projects, to include stealth aircraft, tactical aircraft, space shuttle designs, and even space defense plans. Considered by many to be one of the world's first cyber-attacks against another country, Farewell put the Soviets approximately 15 years behind the U.S. in computers and microelectronics.

In 1997, the Pentagon executed Eligible Receiver, the first information warfare exercise, and determined industrial and information systems throughout the U.S. were vulnerable to cyber-attacks. Using software freely available on the internet, a National Security Agency (NSA) Red Team was able to crack networks and disrupt communications between the National Command Authority, military commands, and intelligence agencies. These vulnerabilities also included multiple power grids and communications networks across the U.S.

The Chinese were believed to have conducted the first state-sponsored cyber-attack against another country in a series of coordinated attacks on American computer systems. The operation was designated as Titan Rain by the U.S. government. The hackers targeted major defense contractor networks in an attempt to gain sensitive information.

The second recorded instance of state-sponsored cyberwar occurred in 2007. During a dispute between Estonia and Russia, massive cyber-attacks against Estonian government agencies, newspapers, and banks forced the shutdown of nearly all Estonian online systems. Though many analysts blamed Russia, a pro-Kremlin youth group took responsibility for the attack. These attacks forced many military organizations to reassess the security of their own networks and the legal ramifications of using cyber-attacks in war.

In 2008, the number of digital devices connected to the internet exceeded the population of earth for the first time. It was also in 2008 that the most significant U.S. military computer security breach occurred, caused by the use of infected flash drives.

Malicious code spread across both the classified and unclassified networks, transferring huge amounts of data to servers under foreign control.

In 2009, Ghost Net, so named by Canadian researchers, was the discovery of a Chinese espionage ring operating on government computers in 103 different countries. That same year, communications links between U.S. ground forces and drones were hacked by Iraqi insurgents.

The number of internet users topped 2 billion in 2010. Also occurring in January 2010 was Operation Aurora, a sophisticated cyber-attack targeting 34 companies in the technology, financial, and defense sectors. Further investigation revealed that the attackers, with ties to both the People's Liberation Army and the Chinese Politburo, used unprecedented tactics that combined encryption, stealth programming, and a previously unknown hole in Internet Explorer to avoid detection systems and obscure their activities.

In June 2010, Stuxnet was discovered. While not the first instance of malware used to attack user systems, Stuxnet was unique in that it was designed to attack computers and networks that met specific configuration requirements. Suspected by many to be a cooperative creation by the United States and Israel to attack Iran's nuclear facilities, Stuxnet demonstrated the robust capability of cyber weapons as a means for causing physical damage to enemy infrastructure.

Although relatively new to our civilization, computers and environment they operate in have become a contested battleground for military operations as well as the backbone of our society. Computers and electronics are included in almost every aspect of our lives, aiding in our ability to communicate and share ideas, shrinking a once large world into a smaller one. It is these aspects that make us vulnerable to those nations or organizations who utilize computers in warfare.

The So What

For over 60 years, the military has been increasing its dependence on digital machines to improve its productivity and its capabilities. We have learned valuable lessons in defensive cyber operations, but until recently, did not incorporate the offensive aspects of cyber into our operations. The military category for cyber is cyber electromagnetic activities (CEMA), defined by ADRP 3-0 as "all activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system."[3] The question, then, is what CEMA is and what purpose does it have in military operations?

Additionally, ADRP 3-0 categorizes CEMA as part of the Mission Command warfighting function. This definition and placement of CEMA appears to be in conflict with the Army Doctrinal Publication (ADP) 6-0's definition of the Mission Command Warfighting Function as "the related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control in order to integrate the other warfighting functions."[4] The definition of CEMA includes "seize, retain, and exploiting an advantage," terms usually associated with an offensive capability, however, it is included as a "task or system" to enable commanders to balance the art of command with the science of control. The conflicts created by these two definitions pose a dilemma for determining cyber's place in military operations . . . is it a Mission Command function or is it a warfighting capability? Or is it both?

We have become adept at defending our cyber networks; however, cyber as an element of combat power is a relatively new concept for U.S. military operations. While Army doctrine has been updated to recognize cyber as a domain and to include cyber electromagnetic activities within military operations, there remain multiple perspectives on how cyber should be used and where that capability should be placed. The current doctrinal placement for cyber electromagnetic activities is within the Mission Command warfighting function. This placement appears to be in direct conflict with the definition of the Mission Command warfighting function, in that it is designed to "develop and integrate," while CEMA involves "seize, retain, and exploit." Additionally, the Mission Command warfighting function contains an identified staff task of "conduct cyber electromagnetic activities," leading one to believe that cyber electromagnetic activities are a staff function.

This thesis will attempt to identify if the Mission Command warfighting function is the correct placement for CEMA by determining the capability that CEMA brings to the battlefield and, more importantly, who it is that is responsible for that capability. If the Mission Command warfighting function is not the correct placement for CEMA, then which of the other warfighting functions would best be suited for CEMA during military operations?

[1] Department of Defense Dictionary, "Cyberspace," http://www.dtic.mil/doctrine/ DOD_dictionary/data/c/10160.html (accessed 28 March 2013).

[2] The National Museum of Computing, "The Colossus Gallery," Codes and Cyphers Heritage Trust, http://www.tnmoc.org/explore/colossus-gallery (accessed 28 March 2013).

[3] Headquarters, Department of the Army (HQDA), Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations* (Washington, DC: Government Printing Office, 2012), 3-3.

[4] Headquarters, Department of the Army, Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: Government Printing Office, 2012), 9.

CHAPTER 2

REVIEW OF LITERATURE

The Cyber Conundrum

Cyber is, and will likely continue to be, an ever-changing environment dependent on emerging technologies and on human innovation. For many years, the military focused primarily on defensive cyber operations in an effort to protect vital command and control systems from unauthorized access. Offensive cyber, while not a new concept, has been thrust into the spotlight due to recent incorporation into military operations by nation states. The consequences of offensive cyber have far ranging effects, from the interception of classified data on one end to the complete disabling of a country's infrastructure on the other. Understanding cyber necessitates visiting some of the terms associated with cyber.

Cyber, as defined by Merriam-Webster, is anything "of, relating to, or involving computers or computer networks."[1] This definition of cyber, while identifying computers as the primary platforms, does not truly capture the man-made operating space where cyber resides. Due to the sheer number of networks that currently exist, and the sheer number of electronic devices that connect to those networks, this man-made operating space has become a new version of the wild west where users cloak their identities and operate with virtual freedom. Cyber exists within an electronic environment, one created by man, and ruled by the technology we currently use within that domain.

DOD, realizing that cyber is not an all-encompassing term in regards to the capabilities resident in each of the services, adopted the term cyberspace in an attempt to capture the physical aspects of cyber, or more importantly, where cyber exists. DOD's definition of cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”[2]

Cyber warfare, as defined by Richard A. Clarke in his Cyber War (May 2010, 6) is the “actions by a non-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption”[3] [to networks or infrastructure]. Clarke’s definition is limited to “actions by a non-state” when in reality many attacks are conducted by state or state-sponsored entities with particular goals in mind. Herbert S. Lin’s definition of cyber warfare is from a legal standpoint, defining offensive cyber operations as “those military operations and activities in cyberspace for cyber-attack against and (or) cyber exploitation of adversary information systems and networks.”[4] Lin’s definition, although mentioning military operations specifically, is broad enough to include all actions that can be taken within the cyber domain to attack anyone considered an adversary, including military, governments, companies, and civilian infrastructure.

Cyberspace, as directed by the 2010 Quadrennial Defense Review[5] and by the National Security Strategy,[6] has become an operational domain in which the military is to conduct operations. This led to the formation of U.S. Cyber Command (CYBERCOM), a sub-unified command under U.S. Strategic Command (STRATCOM), which will lead and coordinate the defense, protection, and operation of DOD networks. This led to the creation of Cyber Electromagnetic Activities, defined as “all activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system."[7]

The Department of Defense Strategy for Operating in Cyberspace (July 2011) offers a unique glimpse at how dependent military operations are on cyber capabilities. "Along with the rest of the U.S. government, the Department of Defense (DOD) depends on cyberspace to function. It is difficult to overstate this reliance; DOD operates over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe. DOD uses cyberspace to enable its military, intelligence, and business operations, including the movement of personnel and material and the command and control of the full spectrum of military operations."[8]

If cyberspace is to be treated as an operational domain, it then follows that cyber has, or at least should have, the characteristics of a domain. The military definition of a domain is the distinct functional area supported by a class of systems with similar requirements and capabilities. Merriam-Webster has three definitions for a domain that appear to apply to military operational domains. These are "a territory over which dominion is exercised," "a region distinctively marked by some physical feature," and "a sphere of knowledge, influence, or activity."[9] For DOD, these domains have typically been identified as land, sea, air, and most recently, space.

So exactly what does cyber electromagnetic activities (CEMA) encompass in this newly designated domain called cyberspace? According to Army Doctrinal Reference Publication (ADRP) 3-0, CEMA activities are those "activities leveraged to seize, retain, and exploit an advantage over adversaries."[10] This would logically lead one to believe that CEMA would include both offensive and defensive capabilities utilized to achieve a military goal or desired end state. Cyberspace operations are “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.”[11] Offensive cyberspace operations (OCO) are defined as “Cyberspace operations intended to project power by the application of force in or through cyberspace.”[12] Defensive cyberspace operations (DCO) are the “passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.”[13]

During the numerous attempts to define both what cyber actually is, what its role will be in military operations, and what the guidelines are for using cyber, additional terms were created to describe cyber operations. Terms such as Information Operations, also encompasses offensive cyber, as “actions taken to affect adversary information systems.”[14] Information Assurance includes the “actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation.”[15] Computer Security, also called COMPUSEC, is “the protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.”[16]

Added to this quagmire of understanding cyber, and the frequent metamorphosis of inter-related terms, are the current legal rules and policies, all of which are as murky as the definition. It is the lack of legal rules and policies, due in part to cyber’s infancy that worries many experts. At the request of the NATO Cooperative Cyber Defense Center of Excellence, The Tallinn Manual was created by a group of international legal experts in an effort to show that the existing laws of war were flexible enough to accommodate cyber.[17] While reflected only an expression of the collection of independent experts, the Tallinn Manual is the result of a three-year effort to determine how international law standards apply to the newest form of warfare. While not an official document of NATO, the Tallinn Manual does address Jus ad Bellum (international law governing the resort to force by States as an instrument of national policy) and Jus ad Bello (the international law regulating the conduct of armed conflict, also known as the law of war).

Warfighting Functions

The warfighting functions exist within military operations as "a group of tasks and systems (people, organizations, information, and processes) united by a common purpose that commanders use to accomplish missions and training objectives."[18] As stated by ADP 3-0, these functions enable commanders to combine art with science to drive the operations process.[19] The warfighting functions include Mission Command, Fires, Intelligence, Movement and Maneuver, Protection, and Sustainment.

The Mission Command warfighting function, as defined by ADP 3-0, "develops and integrates those activities enabling a commander to balance the art of command and the science of control."[20] Under this warfighting function, the commander drives the operations process in order to understand, visualize, describe, direct, lead, and assess the operational environment. ADP 3-0 further states that the commander leads the staff in conducting tasks under the science of control. The four primary staff tasks are to conduct the operations process, conduct knowledge management and information management, conduct inform and influence activities, and conduct cyber electromagnetic activities.[21]

A brief definition of the other warfighting functions, as defined by ADP 3-0 is as follows:

The fires warfighting function as including “the related task and systems that provide the collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process.”[22]

The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations. It includes the synchronization of collection requirements with the execution of tactical tasks such as reconnaissance, surveillance, and related intelligence operations.[23]

The movement and maneuver warfighting function is the related tasks and systems that move and employ forces to achieve a position of relative advantage over the enemy and other threats.[24]

The protection warfighting function is the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission.[25]

The sustainment warfighting function is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance.[26]

As can be seen from the definitions, each of the warfighting functions supports the unit in its own specific way, incorporating the skills of the individual warfighter into a system that supports accomplishment of the mission by converting potential into effective actions, also termed combat power.[27] The commander ties each warfighting function into operational use using the Mission Command warfighting function, enabling the successful convergence of all combat power to a particular place and time on the battlefield.

Conclusions

Compared to the other domains, cyber is still in its infancy. Technology continues to advance, influencing not only cyber's definition, but also cyber's capability within military operations. Currently, the military uses cyber in almost all aspects of operations, and while cyber has indeed increased our productivity, it is a vulnerability that could potentially cripple our ability to respond. To reduce this vulnerability requires awareness of the capability cyber brings to the battlefield.

[1] Merriam-Webster Dictionary, "Cyber," http://www.merriam-webster.com/dictionary/cyber (accessed 2 July 2013).

[2] Department of Defense, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: Government Printing Office, 2007 w/ Change 1, 20 March 2009), GL 7 (CH 1).

[3] Richard A. Clarke, *Cyber War, The Next Threat to National Security and What to Do About It* (New York, NY: Harper Collins, 2010), 6.

[4] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* (August 2010), http://jnslp.com/2010/08/13/offensive-cyber-operations-and-the-use-of-force/ (accessed 10 May 2013).

[5] Department of Defense, *Quadrennial Defense Review Report, February 2010.* http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf (accessed 10 May 2013).

[6] U.S. President, *National Security Strategy, 2010*, The White House, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 12 May 2013).

[7] HQDA, ADRP 3-0, 3-3.

[8] Department of Defense, *The Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf (accessed 12 August 2013).

[9] Merriam-Webster Dictionary, "Domain," http://www.merriam-webster.com/dictionary/domain, (accessed 8 May 2013).

[10] HQDA, ADRP 3-0, 3-3.

[11] Department of Defense Dictionary, “Cyberspace Operations,” http://www.dtic.mil/doctrine/DOD_dictionary/ (accessed 8 May 2013).

[12] Department of Defense (DOD), Joint Publication (JP) 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, 2012), 198.

[13] Ibid., 73.

[14] Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” *The Columbia Journal of Transnational Law* 37 (1999): 885-937.

[15] DOD, JP 1-02, 131.

[16] Ibid., 53.

[17] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, NY: Cambridge University Press, 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual/8?mode=a_p (accessed 31 March 2013).

[18] HQDA, ADRP 3-0, 3-2.

[19] Headquarters, Department of the Army (HQDA), Army Doctrine Publication (ADP) 3-0, *Unified Land Operations* (Washington, DC: Government Printing Office, 2011), 13.

[20] Ibid.

[21] Ibid.

[22] Ibid., 14.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid., 13.

CHAPTER 3

RESEARCH METHODOLOGY

Methodology

While the inclusion of cyber as a defensive component of military operations is not new, attempting to include cyber as an element of combat power is a relatively recent concept for the U.S. military. There are multiple perspectives on how cyber should be incorporated into military operations, but questions remain on where this capability should be placed. Army doctrine has been updated to recognize cyber as a domain and to include cyber electromagnetic activities into military operations, including it under the Mission Command warfighting function. This placement appears to be in direct conflict with the definition of the Mission Command warfighting function, in that it is designed to "develop and integrate," while cyber electromagnetic activities (CEMA) involves "seize, retain, and exploit" terms usually associated with the combat power capabilities included in other warfighting functions. An identified staff task of "conduct cyber electromagnetic activities" also exists within the Mission Command warfighting function, leading one to believe that cyber electromagnetic activities are a staff function.

The primary research method used during this thesis is a qualitative examination of multiple DOD and non-DOD sources related to cyber, CEMA, and Mission Command. These sources include doctrinal publications, journals, articles, and internet sources relevant to the use of cyber, CEMA, and Mission Command within the military. Other qualitative techniques utilized during this examination included informal discussions with military leaders, briefings, and interviews with subject matter experts. This information is intended to aide in exploring the terms related to cyber, CEMA, and Mission Command, and in establishing definitions, roles, and capabilities pursuant to those terms.

Basic research methods included within this study encompassed the examination of current definitions and terms for cyber electromagnetic activities and Mission Command, primarily focusing on the roles each has in the operations process. Cyber and the other warfighting functions were also briefly examined. This information is critical in establishing basic terms and definitions, and lends relevance to how the Army defines the roles of cyber, CEMA, and Mission Command in both current and future military operations.

Goals and Expected Outcomes

Debate continues regarding both cyber's place in military operations and what cyber will bring to the fight. The goal of this thesis is to further facilitate the discussion and understanding of cyber within military operations, to include its placement, role, and capabilities by identifying why CEMA has been placed within the Mission Command warfighting function. Exploring the doctrinal definition of cyber, CEMA, and Mission Command is expected to lend relevance and understanding to both CEMA and the Mission Command warfighting function for military leaders.

Research Topics

While there are multiple topics related to the discussion of cyber within military operations, this research paper focused primarily on those topics relating to cyber, CEMA, and the Mission Command warfighting function. The following topics will be defined and explored in order to facilitate understanding.

Cyber, cyber domain, and cyberspace will be defined and explored to ensure understanding of the "cyber" concept and to identify the base capability that cyber operations bring to military operations.

"Cyber electromagnetic activities" is the Army's term for cyber. This term will be defined using current doctrinal definitions, to include cyberspace operations, Electronic Warfare, and Electromagnetic Spectrum Operations. It is expected that defining CEMA and the capabilities each of its three components offers to the warfighter will identify not only what the Army expects of CEMA operations, but will offer some insight as to where CEMA operations should be placed within military operations.

An examination of the meaning and purpose of a warfighting functions is expected to lend relevance to the discussion on which warfighting function should contain CEMA, and whether the Mission Command warfighting function is the correct placement for CEMA.

The Mission Command warfighting function will also be examined in order to determine exactly what the Mission Command warfighting function does, or is expected to do, in military operations. This examination is expected to identify whether the current placement of CEMA within the Mission Command warfighting function is correct, or if that placement has created conflicts that may inhibit operations.

Applied Questions

Two basic questions were posed for each topic, and in some cases subtopics, in order to facilitate an understanding of the terms, definitions, roles, and capabilities of the topic. In the case of this thesis, "topic" refers to those topics related directly to the discussion of cyber, CEMA, and Mission Command. These questions are as follows:

How is it defined?–This question addresses the basic definition of the topic and what equipment, processes, or components make up the topic. Definitions to be explored will be kept as close to current doctrinal definitions as possible.

What is its purpose?–This question focuses on what the topic's role is, or what it is intended to accomplish, within military operations.

It is also expected that an exploration of the answers to these questions will lead to the identification of any gaps in the understanding, doctrine, or in the applied usage of cyber, CEMA, and Mission Command. A brief exploration using these same questions will be applied to other warfighting functions, but that exploration is not expected to encompass the full capabilities or duties of those warfighting functions.

Discussion

It is expected that a final discussion of terms will then follow the two basic questions, leading to the further identification of conflicts that may, or may not exist, between cyber, CEMA, and Mission Command. During this discussion, each of the major terms will be examined and compared to the other terms. Additionally, a comparison of terms is expected to identify any areas requiring further clarification or study to accurately solve the research question.

It is expected that this discussion will lead to the identification of answers to the primary research question of why CEMA is placed within the Mission Command warfighting function. Additionally, the discussion is also expected to answer the following secondary research questions:

What is the capability that cyber/CEMA brings to the battlefield and who is responsible for that capability?

If the Mission Command warfighting function is not the correct placement for CEMA, then which warfighting function is the correct place for CEMA in military operations?

Weaknesses

This thesis is unclassified, and as such, will be based on available information that is also unclassified. While this information will include both DOD and non-DOD sources, it is acknowledged that the amount of relevant information regarding cyber, CEMA, and Mission Command is vast and complex. Policies and procedures regarding cyber and its use within the military continue to be updated and changed as its role and capabilities are refined. Additionally, it is further acknowledged that these policy changes are also affected as information changes due to updates and revisions. This thesis focuses on information gleaned by the researcher as of 15 October 2013, which admittedly does not cover all cyber references or sources currently available. This information may or may not be considered outdated or irrelevant to future readers, but is expected to lend relevance to the overall discussion of cyber within military operations.

A second identified weakness in this thesis is also related to the information referred to in the previous paragraph. There exists a vast amount of information on early, current, and expected uses for both cyber and Mission Command. Attempting to include all available information within the time required to complete this research project was impractical. It is acknowledged that further relevant information may exist which may, or may not, have an impact on this thesis or on the discussion of cyber within the military.

Lastly, it is also acknowledged that cyber within the U.S. military is relatively new in comparison to other weapon systems. As such, cyber is continuing to change and adapt as it is molded into our operations. As such, this thesis focuses narrowly on cyber within the Mission Command warfighting function, a scope that does not encompass all CEMA operations, cyber operations, or other aspects of cyber within military operations.

CHAPTER 4

ANALYSIS

Defining the Terms

The military has a term or phrase for almost everything that exists, to describe not only the actions, but also the expected outcomes for systems, processes, and equipment. These terms and phrases are important as they aid in the rapid understanding of capabilities and processes by the professional Soldier. Terms can also cause confusion when new systems, processes, and equipment resemble the older systems, processes, and equipment still in use, or when there is an attempt to use existing systems to conduct seemingly new operations. Understanding the definitions of these terms, aids in determining what a system or process is meant to accomplish, identifying its purpose in regards to the processes towards which that term is used. In the case of cyber electromagnetic activities (CEMA), understanding the definition of CEMA aids in identifying what it is that CEMA is intended to accomplish within military operations. The following pages will explore the terms and phrases relevant to cyber, CEMA, warfighting functions, and Mission Command in order to determine doctrinal definitions and to establish an understanding of those terms. As an additional note, terms and phrases have been kept as close to military doctrinal definitions as possible to ensure transparency.

Cyber

How is it Defined?

Cyber, as a definition, includes anything having to do with computers and the networks that connect them together.[1] This definition is vague in that it limits cyber to computers and does not encompass newer electronic devices that connect to the network to send and receive data. Wireless phones, printers, and cameras, to name a few, all connect to the network to send and receive data, effectively creating a separate dimension consisting of networks, devices, and communications that redefines our operational environment. In essence, these devices have been "computerized" in that they transmit, receive, and process data in the form of electronic energy over a network. A better definition to explain this cyber phenomenon might be anything having to do with computerized devices capable of connecting to networks and the networks that enable them to share data.

What is its Purpose?

One of the original purposes of cyber in military operations was to increase productivity within an organization. Computers and the networks upon which they operate enable military command structures through the rapid availability of information between organizations. The use of electronic mail (email) has increased communications and collaboration efforts at all levels, while the use of video teleconferencing (VTC) enables personnel from different sides of the globe to conduct conferences in real-time.

Computers are also used to store and share data across vast distances, increasing the exploitation and information collection efforts. When data is collected together with other data, it can then be arranged to have meaning. This meaning is referred to as information. The sharing of data across multiple organizations through multiple networks increases the amount and validity of the information available to the organization. This same sharing, however, also increases the risk that data can be influenced, or changed, by enemies of the organization, causing the information to become invalid.

Cyber Domain

How is it Defined?

The cyber domain is an operating area that exists electronically; an environment composed of electronic data moving faster than thought. What sets the cyber domain apart from the other natural domains (air, land, sea, and space) is that the cyber domain is a completely man-made domain consisting of physical, logical, and social layers.[2]

The physical layer comprises geographical and physical components that support the network. This layer includes the geographic location, such as air, land, sea, or space where portions of the network exist, as well as components such as the hardware, software, infrastructure, and physical connections. Without this physical layer, the other layers cease to function.

The logical layer, sometimes referred to as the syntactic layer, consists of the software that provides the operating instructions for the physical equipment. These instructions provide the procedures, in the form of code, that the physical equipment uses to transfer and receive data across the network.

The final layer, the social layer, also called the sematic layer, involves human interaction. This layer is made up of the persona and cyber persona components of the users and their interaction with the information produced by computers, as well as the way that the information is interpreted by those users.

Whereas the environmental rules that apply to the other domains are defined by nature, the rules for cyber, as a domain, are defined by programming codes and security protocols. These cyber "rules" determine how the network will exist, what data can be transferred on the network, and what other networks can connect to the network. These same rules also determine the strengths and weaknesses of a network.

Cyberspace, yet another term synonymous with "cyber domain," is a word adopted from science fiction literature in the 1980s. This is yet another attempt to describe the electronic environment upon which computers operate, and more importantly, to explain the global impact cyber has in the interwoven electronic environment. Cyberspace encompasses the aggregate of every connected network and device around the world, a massive web of electronic connections and interwoven pathways existing through hardwired cables and across the electromagnetic spectrum. The military definition of cyberspace is as a global domain within the information environment that consists of computers and computer networks.[3] Key to this definition is the mention of the term information environment, or the aggregate of individuals, organizations, and systems that collect, process, disseminate or act on information.[4] By these two definitions, cyberspace is the intersection of two environments, the electronic environment and the information environment.

A key concept to understanding the cyber domain is that it turns information into a commodity. Information is data that has been collected, sorted, and processed to have meaning. This data and information has always existed, yet with cyber and the cyber domain, data and information from around the world can be accessed with the click of a button. The more data one has access to leads to additional and improved information; additional information leads to the ability to create better plans and make better decisions.

What is its Purpose?

The cyber domain is a man-made domain of interwoven and interconnected networks and computers. The primary purpose of the cyber domain is to facilitate communication and data sharing using computers and communication networks. This amplified communication improves the ability of the commanders and staffs to understand the battlefield environment and to rapidly and clearly transmit their orders, thus more effectively exercising command and control. Adversely, by attacking cyber networks, one can degrade understanding and hinder the exercise of command and control. An additional characteristic that enables cyber operations is in the planning for cyber. The expansive nature of the cyber domain enables planners to focus on the effects versus the means to create those effects. For instance, if the planned effect is to degrade information, cyber leverages the choice of multiple targets and offers multiple means by which to achieve that effect.

Cyber Electromagnetic Activities

How is it Defined?

The current military term for cyber is cyber electromagnetic activities (CEMA). Cyber electromagnetic activities are all activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.[5] CEMA consists of three components:

cyberspace operations, electronic warfare, and electromagnetic spectrum operations.[6] These three activities employ the same technologies, capabilities, and enablers to accomplish assigned tasks.

What is its Purpose?

CEMA acts as an enabler to the operations process in that it protects and sustains communication networks while providing a platform from which users can securely interact, share information, exchange ideas, and communicate. Additionally, CEMA provides a means, using Electronic Warfare (EW) and cyberspace operations, with which information, or more specifically the data that makes up information, can be further influenced. ADRP 3-0, paragraph 3-5 states that every operation requires cyber electromagnetic activities to ensure information availability, protection, and delivery as well as a means to deny, degrade, or disrupt the enemy's use of its command and control systems and other cyber capabilities.[7]

CEMA is the activities leveraged to seize, retain, and exploit an advantage over adversaries in both cyberspace and the electromagnetic spectrum, but what exactly is it that CEMA is affecting? All three components of CEMA are inter-related in both definition and the platforms they use. Cyberspace operations are conducted to protect and influence information, using electronic signals sent through networks. EW uses electronic signals to protect, defend, and support the use of the electromagnetic spectrum. Electromagnetic Spectrum Operations (EMSO) manages and mitigates the use of electronic signals within the electromagnetic spectrum. Comparatively, all three rely upon the use of electronic signals sent through the electromagnetic spectrum and all three have a direct effect on data in "seizing, retaining, and exploiting" advantages over adversaries. As data is the smallest aggregate of information, and information is of utmost importance in military operations, it can be argued that CEMA's purpose then is to influence and protect this data through cyberspace operations and the use of radio signals. This is the basic capability CEMA brings to the battlefield, the ability to influence and protect information by influencing and protecting data.

Cyberspace Operations

How is it Defined?

Cyberspace operations are those actions conducted in and through cyberspace that inherently influence an operational environment. These operations can be further broken down into offensive and defensive tasks. Offensive tasks, as defined by ADP 3-0, are tasks conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers.[8] Defensive tasks are those that are conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks.[9]

What is its Purpose?

In regards to cyberspace operations, an offensive task would be a task conducted in the cyber domain intended to seize, retain, or exploit an enemy network or information system. Conversely, defensive tasks would be those that are conducted to prevent the enemy from disrupting friendly military operations. The purpose of both offensive and defensive cyberspace operations is to support the military operation.

Electronic Warfare

How is it Defined?

Electronic Warfare (EW), a concept developed during the Cold War with the Soviets to prevent the disruption of U.S. military communications, declined during the 1990s due in part to the decline of the Soviet Union. It reemerged during the Iraq and Afghanistan wars as part of the strategy for defeating improvised explosive devices (IEDs) used against U.S. forces. Due to the IED's cheap cost and effectiveness, military officials see the use of IEDs as an enduring threat to U.S. forces operating world-wide. As part of CEMA, electronic warfare has emerged once again as an important capability in protecting Soldiers and defeating IEDs. EW uses electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum. Newer technologies have enabled EW to incorporate wireless technologies, high-power microwave, directed energy, and electro-optical devices that act as enablers to expand current networks.[10]

What is its Purpose?

According to Field Manual (FM) 3-36, EW is one of "2 lines of effort in cyber electromagnetic activities" and consists of three divisions: electronic attack, electronic protection, and electronic warfare support.[11] Electronic attack is the use of electromagnetic energy, directed energy, or anti-radiation weapons to prevent or reduce the enemy's effective use of the electromagnetic spectrum. Defensive electronic attack activities use the electromagnetic spectrum to protect personnel in cases such as the emergence of IEDs. Electronic protection involves those actions taken to protect against the effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.[12] Electronic protection also includes electromagnetic spectrum management in the coordination and deconfliction of spectrum resources.[13] The third division of EW, electronic warfare support, involves actions tasked by the commander to identify and locate intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, and planning.[14]

Electromagnetic Spectrum Operations

How is it Defined?

Electromagnetic spectrum operations (EMSO) is a concept that incorporates spectrum management, frequency assignment, policy implementation, and host nation coordination to enable the commander's use of the electromagnetic spectrum.[15]

Spectrum management is the identification and mitigation of environmental effects on military radio frequencies and managing those frequencies to remove conflicts between military radio systems and host nation civilian radio systems. Frequencies are then assigned and controlled for military units to ensure command and control capabilities. Host nation coordination must occur as each nation has sovereignty over the electromagnetic spectrum within its borders.

What is its Purpose?

EMSO is an enabler for military operations, supporting the warfighter's use of the communications network through the electromagnetic spectrum. The electromagnetic spectrum is a finite resource with multiple competing entities and networks attempting to use that resource at the same time. EMSO manages the electromagnetic spectrum by identifying spectrum requirements, coordinating spectrum use, and ensuring the efficient use of the spectrum.

Warfighting Functions

How is it Defined?

FM 3-0 introduced the warfighting functions as a replacement for the Battlefield Operating System. A warfighting function is a group people, tasks, and systems united by a common purpose that commanders use to accomplish missions. Warfighting functions are also used to generate combat power by converting potential into effective action. Another key characteristic of a warfighting function is that it exists across domains. For example, the fires warfighting function can execute targets on the ground, in the air, and at sea. What fires does in their targeting and execution processes are the same across all three of these domains.

What is its Purpose?

Each of the warfighting functions serves a particular role in generating combat power for the commander and each has been refined through use and analysis to provide the tasks and systematic approaches required for successful contribution to military operations. The fires warfighting function is the related task and systems that provide collective and coordinated use of Army fires, air and missile defense, and joint fires through the targeting process. The tasks and systems that facilitate the understanding of the enemy, terrain, and civil considerations define the intelligence warfighting function. The movement and maneuver warfighting function relates to the tasks and systems that move and employ forces to achieve positions of advantage over the enemy and other threats. The protection warfighting function is the related tasks and systems that preserve the force while the sustainment warfighting function provides the support and services to ensure freedom of action, operational reach, and endurance. The mission command warfighting function serves a dual role in that it develops and integrates the other warfighting functions to enable the commander to balance the art of command with the science of control.

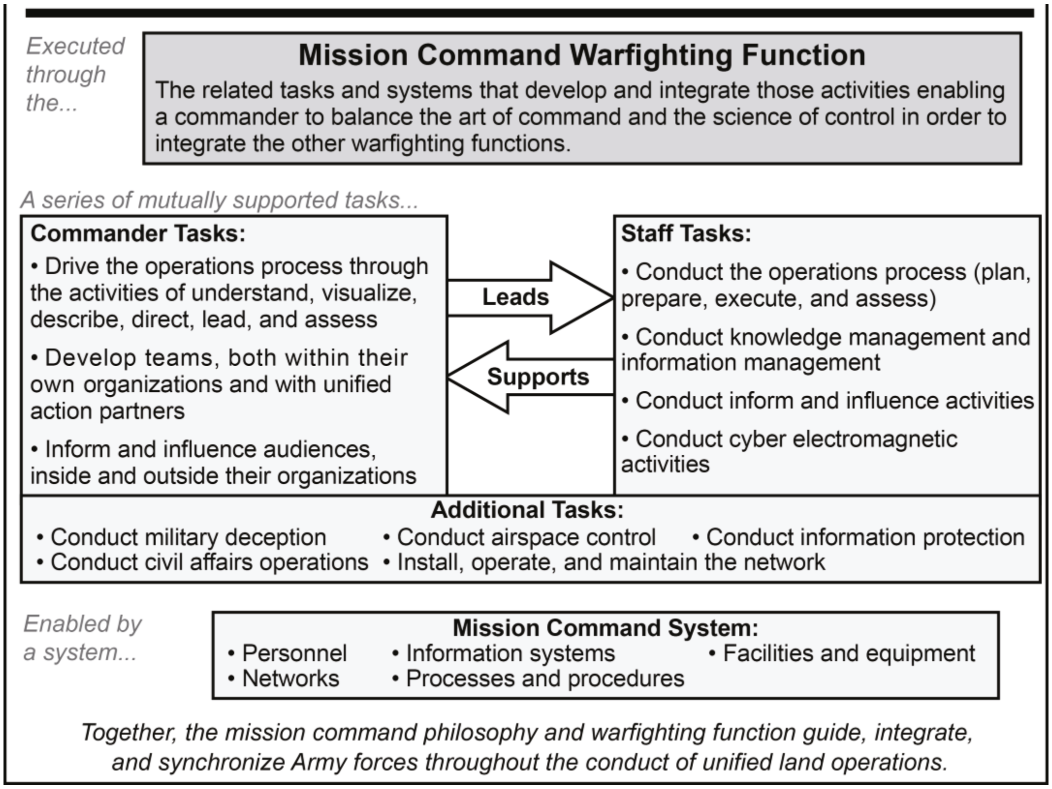
The Mission Command Warfighting Function

How is it Defined?

ADP 6-0 describes the Mission Command warfighting function as tasks and systems that enable the commander to balance the art of command and the science of control in order to integrate the other warfighting functions. The Mission Command warfighting function is a combination of mutually supported tasks, led by the commander and supported by the staff, which supports the commander's exercise of authority through the decentralized execution of mission type orders. These tasks and systems integrate the other warfighting functions, massing their effects to focus at the crucial place and time on the battlefield.

What is its Purpose?

Commanders perform three primary tasks under the Mission Command warfighting function, drive the operations process, develop teams, and inform and influence audiences. The operations process aids commanders in translating decisions into action and synchronizing forces. Commanders develop teams to exchange ideas and to synchronize efforts, as teams are crucial to success, while informing and influencing activities support the commander’s operational goals. Figure 1 displays the lower half of the chart on page IV of APD 6-0, titled the Exercise of Mission Command, and defines Mission Command as a warfighting function consisting of mutually supported tasks. The commander tasks lead the staff tasks and staff tasks support the commander’s tasks, creating a continuous cycle in which the commander leads and the staff supports.



Executed through the...

Mission Command Warfighting Function

The related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control in order to integrate the other warfighting functions.

A series of mutually supported tasks...

Commander Tasks:

- Drive the operations process through the activities of understand, visualize, describe, direct, lead, and assess
- Develop teams, both within their own organizations and with unified action partners
- Inform and influence audiences, inside and outside their organizations

Staff Tasks:

- Conduct the operations process (plan, prepare, execute, and assess)
- Conduct knowledge management and information management
- Conduct inform and influence activities
- Conduct cyber electromagnetic activities

Additional Tasks:

- Conduct military deception
- Conduct airspace control
- Conduct information protection
- Conduct civil affairs operations
- Install, operate, and maintain the network

Enabled by a system...

Mission Command System:

- Personnel
- Information systems
- Facilities and equipment
- Networks
- Processes and procedures

Together, the mission command philosophy and warfighting function guide, integrate, and synchronize Army forces throughout the conduct of unified land operations.

Figure 1. Mission Command Warfighting Function Model

Source: Headquarters, Department of the Army, Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: Government Printing Office, 2012), iv.

The commander’s task of “drive the operations process through the activities of understand, visualize, describe, direct, lead and assess” leads the staff task of “conduct the operations process (plan, prepare, execute, and assess). This staff task then supports the commander's task of "drive the operations process through the activities of understand, visualize, describe, direct, lead and assess." The same cycle can be applied to the commander's task of "inform and influence audiences, inside and outside their organization." This task, when applied to the staff, supports the commander as the staff "conducts inform and influence activities."

The commander also has a commander specific task to "develop teams, both within their own organizations and with unified action partners." No staff tasks are identified to aid the commander in conducting this task, yet it is expected that the staff supports the commander as he or she builds the staff into a cohesive team within the organization.

The staff tasks also contain two tasks that are not identified as commander tasks. The first, "conduct knowledge management and information management," while not identified as a commander task, is a task that supports the commander's task of "drive the operations process." Knowledge and information management aid in providing the commander the information needed to create and maintain understanding to make effective decisions. The other staff task that is not identified as a commander task is "conduct cyber electromagnetic activities." ADRP 3-0, paragraph 3-14, states that commanders integrate and synchronize cyber electromagnetic activities across all command echelons and warfighting functions as part of the operations process. ADP 6-0, paragraph 43, assigns this same task to the staff, to integrate and synchronize cyber electromagnetic activities across all command echelons and warfighting functions.

Five additional tasks are nested at the bottom of the commander tasks and staff tasks. These tasks are conduct military deception, conduct airspace control, conduct information protection, conduct civilian affairs operations, and install, operate, and maintain the network. The nesting of these tasks depicts their importance in operations and reinforces the influence the commander and staff have on conducting these tasks.

The last box in the chart, titled Mission Command System, depicts the enablers of the Mission Command warfighting function. These enablers are personnel, information systems, facilities and equipment, networks, and processes and procedures. Enablers are best described as critical functions, processes, or equipment that facilitates an organization to accomplish an objective.

As an additional note, ADPR 6-0, para 1-15 states, "by itself, the mission command warfighting function will not secure objectives, move friendly forces, or restore essential services. It provides purpose and direction to the other warfighting functions to help achieve objectives and accomplish missions."

CEMA and the Mission Command Warfighting Function

Joint Publication (JP) 1-02 defines a capability as "the ability to execute a specified course of action." A capability is designed through force structure, modernization, readiness, and sustainability to deliver a specific "effect" on the battlefield. By this definition, and the earlier definition of CEMA, CEMA provides two capabilities on the battlefield, the capability to protect and influence information and the capability to operate on the electromagnetic spectrum. While there is an argument that cyberspace operations provide a capability that has a direct effect on enemy electronic devices, a counter argument can be made that this effect is still made on the information the device uses for operation. For instance, cyberspace operations could be conducted to increase the amount of water allowed to flow out of the dam while also forcing the valve to depict an erroneous reading in the control room. The direct effect, in this case, is to change the output flow and change the valve reading. The counter to this argument is that data is sent through a computer to whatever device is controlling the output. This output device requires information (in the form of code) to make changes to the flowing water, as well as information (again in the form of code) to provide the erroneous reading view in the control room.

Having identified what it is that CEMA brings to military operations in the way of capabilities, the question that then must be asked is where should CEMA exist in the military operations process and how to operationalize that capability?

An obvious answer would have been to create a separate warfighting function to include CEMA, a warfighting function that encompassed the offensive and defensive tasks of cyberspace operations, electronic warfare, and spectrum management. The definition of a warfighting function is “a group tasks and systems united by a common purpose,” “used to generate combat power by converting potential into effective action.” CEMA meets the first part of this definition as all three components of CEMA are interrelated; use similar platforms in conducting their operations, work within the cyber domain, and all work towards the same goal of protecting or degrading information. It is the second part of a warfighting function definition that requires further examination.

A warfighting function is used to generate combat power by converting potential into effective action. Combat power is the “total means of destructive, constructive, and information capabilities that a military unit or formation can apply at a given time.”[16]

CEMA's capability is to protect and influence information. For CEMA to become its own warfighting function CEMA would have to convert potential, in this case information, into effective action. The question then turns to the information, or more specifically, who determines what information is required, what role that information will have in operations, and who fulfills those information requirements?

Information is data that has been collected, processed, and shared to convey a specific message. This information, in the case of military operations, is used to create a visualization and understanding of what is about to occur, or is occurring on the battlefield. The answer to the question of who determines information requirements and its role in military operations is the commander. The commander operationalizes information by determining what information he requires and for how long he requires that information. The commander is the one who defines the variables for information into measureable factors and uses the information to make informed decisions on how best to apply combat power. This is how information becomes an element of combat power, how it is operationalized into military operations. CEMA's part in this operationalization process is to protect information, and in some cases, degrade the enemy's use of information at the discretion of the commander.

CEMA by its definition protects the availability of information while providing a means to degrade the enemy's use of information. The key point here is that CEMA does not provide information; it protects it or degrades it. CEMA simply protects the network through which data flows, enabling the collection, storage, and processing of data into information. Collection, storage, and processing of data into information is a human process created through design. If the collection, storage, or processing designs are faulty, then the information will also be faulty. An analogy would be a water pipe. The water exists at point A, but you exist at point B. To get the water from point A to point B you use a pipe, thus enabling you to move the water to your current location. At one end, you include a filter to remove water impurities and at the other, you install a basin to hold the water. CEMA's purpose in this process is to act as the filter and protects the pipe (the network) through which data (factoids that exist without meaning within the cyber domain) flows. As long as the pipe is connected to the network, data will flow back and forth. The data flowing through the pipe has no real meaning until it is collected and processed by humans into a relevant message, which we call information. Similarly, CEMA offers the capability to negatively influence the flow of information. By influencing the size of the pipe available for the enemy to use, you influence the amount of data that can be gathered, thus restricting the information process. Additionally, introducing faulty data into the enemy's pipe potentially produces faulty information.

Humans, in the form of the staff, the other warfighting functions, and the subordinate units provide information to the commander, shaping it to meet his or her requirements to support the commander in using that information. Cyber and CEMA may have an effect on information by protecting and providing the platform (in this case the network), but they do not determine what information is relevant nor do they process the data into information. If it is the commander that operationalizes information and the staff who collects and shapes it, then CEMA's role in the information process remains as an enabler. This precludes CEMA from ever being a warfighting function.

So if CEMA cannot be its own warfighting function, where then should it be placed as a capability within military operations? If it is the commander who operationalizes information by turning it into an element of combat power using the Mission Command warfighting function, and CEMA provides the capability to protect and influence information, then it is only logical to include CEMA within the same warfighting function that the commander leads. Additionally, the Mission Command warfighting function already contains the tasks for install, operate, and maintain the network, conduct information protection, knowledge management, information management, and inform and influence activities . . . all of which are tasks closely related to CEMA operations.

Including CEMA, and more importantly the capability to influence information, within the Mission Command warfighting function also ensures that the commander is involved in information as an element of combat power, and that the commander is able to make decisions, both informed and timely, despite the uncertainty of the environment he finds himself in.

Accepting that CEMA should be included within the Mission Command warfighting function poses yet another question. Where within that warfighting function should CEMA exist? There is a staff task of “conduct cyber electromagnetic activities” that leads one to believe that the staff conducts CEMA activities. While there is agreement that some parts of the staff, the S6, Knowledge Manager, and even the Information Security Officer use computers for “information protection and influence activities,” is the staff truly conducting CEMA activities? The answer to this question is ambiguous and lays both in the supporting role the staff has with the commander and with the labeling of the staff task “conduct cyber electromagnetic activities.” The entire staff does use information systems and processes to gather and develop information for the commander to use in decision-making; however, there are only a select few staff members who are actually engaged in the doctrinal CEMA tasks of Cyberspace Operations, Electronic Warfare, and Electromagnetic Spectrum Operations. It can be argued that the staff task of “conduct cyber electromagnetic activities” in this case, is mentioned more as a “concept” to protect and influence information, and not as a doctrinally CEMA defined task. The task is similar to CEMA in that the staff protects and directly influences information in support of the commander, but is different in that it is not a cyberspace, electronic warfare, or spectrum management task. It can be further argued that this staff task of “conduct cyber electromagnetic activities” is an enabler and is already included in the networks, information systems, processes, and procedures included within the Mission Command system.

[1] Merriam-Webster Dictionary, “Cyber.”

[2] Paul Rosenzweig, “Cybersecurity, An Introduction,” *Hoover Institution Journal*, 2011, http://www.hoover.org/publications/defining-ideas/article/93736 (accessed 13 June 2013).

[3] Department of Defense Dictionary, “Cyberspace.”

[4] DOD, JP 1-02, 131.

[5] HQDA, ADRP 3-0, 3-3.

[6] Note: ADRP 3-0, dated May 2012, defines CEMA to include three components, cyberspace operations, electronic warfare, and electromagnetic spectrum operations. FM 3-36, dated November 2012, identifies two of these components as “lines of effort.” It is inferred from these definitions that electromagnetic spectrum operations are not a “line of effort” but are considered a supporting effort.

[7] HQDA, ADRP 3-0, 3-5.

[8] HQDA, ADP 3-0, 5.

[9] Ibid.

[10] Headquarters, Department of the Army (HQDA), Field Manual (FM) 3-36, *Electronic Warfare* (Washington, DC: Government Printing Office, 2012), 1-1.

[11] Ibid., 1-3.

[12] Ibid., 1-5.

[13] Ibid.

[14] Ibid., 1-6.

[15] Headquarters, Department of the Army (HQDA), Field Manual (FM) 6-02.70, *Army Electromagnetic Spectrum Operations* (Washington, DC: Government Printing Office, 2010), 1-1.

[16] HQDA, ADRP 3-0, 3-1.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

The cyber domain grew from the advent and improvement of the computer. This domain currently has approximately 1.1 billion computers operating inside it with few policies and pacts by which all countries agree to abide in regards to cyber activities. Computers, and thus cyber, exists almost everywhere in current military operations, bringing communications networks to the battlefield as well as the ability to conduct operations in the electromagnetic spectrum. Cyber is a multiplier to our operations, enhancing our ability to operate across the other domains. Each of the other domains can exist without cyber, and we can conduct operations in those domains, but without the cyber domain, those operations would be greatly diminished.

Cyber's base capability is to send and receive data. This data, when compiled with other data, can be formed into information. This data can also be altered within the cyber domain, thereby influencing the information that is formed from the data. Cyber electromagnetic activities (CEMA) is the Army's "capability" to affect that information on and through the cyber domain.

CEMA, due to its "base" capability, requires a place in military operations where it becomes a part of the "information process," the process where data is refined, collected, and shaped into information. CEMA does not provide that process, but is a part of that process in that it ensures information integrity, or in the case of the enemy information process, degrades that integrity, by influencing the data that makes up the information.

Cyber cannot become a separate warfighting function, at least not until it has reached some level of maturity. Cyber operations are relatively new, and so are many of the activities conducted by CEMA. The definition for a warfighting function contains "tasks and systems," inter-connected activities that form a set of procedures, influencing how and what the group does every time. CEMA's definition contains "activities," a collection of people and actions to reach a singular desired goal, one that may change with every operation. Cyber, and thus CEMA, is too new to have established tasks and systems and the military is just now addressing certain cyber procedures. Add to this that cyber operations, specifically the use of computers, occurs within every aspect of military operations, and more importantly, within each of the other warfighting functions. Attempting to separate these "cyber operations," to classify them as separate "tasks and systems" from the other warfighting functions, would greatly diminish current military capabilities and inhibit those warfighting functions from generating the maximum amount of combat power possible for the commander's use.

An additional problem that would arise in creating a separate "CEMA warfighting function" would be that it would inhibit military operations by effectively removing the commander from the information process. The commander is the one who turns information into an element of combat power by determining information requirements within the unit. For CEMA to become a separate warfighting function would require that CEMA turn potential, in this case data, into effective action, thereby generating combat power. If CEMA were to determine data and information requirements, the commander would be "force-fed" information that may or may not be relevant, impacting his ability to make informed decisions.

The primary purpose of Mission Command is to accomplish the mission through the generation of combat power, or the total destructive and/or disruptive force that a military unit/formation can apply against the opponent at a given time. CEMA, then, is the Army’s “information combat power,” protecting and influencing information through the cyber domain and across the other domains. The commander is the driving force in information development, utilizing the Mission Command warfighting function to drive information requirements and priorities, then using that information to make and implement decisions.

The primary purpose of CEMA is to influence and protect information. Cyber electromagnetic activities belong within the Mission Command warfighting function based upon CEMA’s capability to protect and influence information and upon the primary use for which information is used, to support the commander’s ability to make timely and informed decisions.

Cyber, and CEMA, will continue to mature based upon advances in technology and upon doctrinal refinement, changing not only what we can accomplish in cyberspace, but also how we do it. For now, CEMA’s placement within the Mission Command warfighting function is due to the capability CEMA has in protecting and influencing information, acting as an enabler not only to communications, but also to information development.

Methodology

While the methodology used during this thesis is only “one way” of reaching the following conclusions, it is expected that utilizing other methodologies to conduct the same research would yield similar results due in part to cyber’s relative infancy in military operations. Looking at the same research question from a joint, interagency, or even from a multinational point of view would likely yield the same result; that cyber, and therefore CEMA, is an enabler to military operations in and through cyberspace. This capability requires direct commander input to identify required information in order to operationalize information into the operation. It is expected that any attempt to define the capabilities of cyber, CEMA, and Mission Command using any methodology would lead the researcher to similar conclusions.

Information and the Cyber Domain: The Real Issue

It must be acknowledged that cyber is only a part of CEMA, one currently subject to large-scale discussion as to capabilities and implementation policies due to its relative infancy. The real issue, however, is not about cyber, or CEMA, within our operations, it is about the information in our operations.

Information is the vital commodity at every level of every military operation. This information is used to create an effect on the battlefield or used to increase influence with our allies. While it is agreed that cyber does enhance the processing and collection of data into information, this information would still exist without cyber, similar in that the air domain would continue to exist without the airplane. If one were to remove the airplane, or any of the other machines capable of flight from the air domain, the natural laws that make up the air domain would continue to remain unchanged by their removal. This same experiment can be applied to the land, sea, and space domains. The use of machines within these domains is nothing more than a capability that we use in achieving mastery over our opponents.

This same analogy can be applied to the cyber discussion, and more importantly, to the question of cyber as a true domain. If we look at the computer as a tool used to access a domain, similar to the airplane accessing the air domain, the answer of cyber being a true domain is obvious. The computer is the user's access point to the cyber domain. If we remove the computer, does the cyber domain still exist? Since cyber's definition is having to do with computers, the obvious answer is no. Without the computer, the cyber domain cannot exist, nor can the networks that have become a part of the cyber domain.

Cyber is a capability in that it enhances our ability to achieve information superiority. This information would continue to exist if cyber efforts were removed, it would just be harder for us to collect and process the information. Information, then, should be our focus, and information should be the domain upon which we operate. It is information that is applied at the correct time and place to achieve a desired goal. Cyber, and thus CEMA, are merely part of the information process in that they enable the collection and processing efforts. Cyber proponents will argue that cyber can achieve an effect by directly influencing electronic equipment, such as water valves in a dam. While this argument is valid, the counter argument is also valid, in that it is information that is sent from the computer to the water valve that causes the water valve to malfunction.

Cyber is an electronic environment upon which flows data. CEMA is the title given to the three components (cyberspace operations, electronic warfare, and electromagnetic spectrum operations) that make up our capability to protect or influence information. Cyber and CEMA are tools used during military operations to achieve information superiority on the information domain, not on the cyber domain.

Questions for Future Researchers

During the course of this thesis, several questions arose that may, or may not, have an impact on the discussion of cyber, CEMA, and Mission Command. These questions offer an insight to the complexity of cyber within military operations, and are included here as recommendations for further research.

The military's goal during operations is to attempt to gain control and mastery over the various domains, furthering our own freedoms and degrading the enemy's ability to conduct operations. This control and mastery enables the military to dictate what the enemy can or cannot do within those domains. Due to the current size of the cyber domain, is it possible to achieve cyber domain superiority?

If CEMA's main purpose is to protect and influence information through tasks conducted on the cyber domain, and cyber is anything having to do with computers, and computers are used to send, receive, and store information, then should the cyber domain actually have been named the information domain? Is the concept of an information domain really something new?

BIBLIOGRAPHY

Government Documents

Department of Defense. Joint Publication 1, *Doctrine for the Armed Forces of the United States.* Washington, DC: Government Printing Office, 2013.

______. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, DC: Government Printing Office, 2011.

______. Joint Publication 3-13, *Information Operations.* Washington, DC: Government Printing Office, 2012.

______. Joint Publication 6-0, *Joint Communications System.* Washington, DC: Government Printing Office, 2010.

Headquarters, Department of the Army. Army Doctrine Publication 3-0, *Unified Land Operations.* Washington, DC: Government Printing Office, 2011.

______. Army Doctrine Publication 6-0, *Mission Command.* Washington, DC: Government Printing Office, 2012.

______. Army Doctrine Reference Publication 3-0, *Unified Land Operations.* Washington, DC: Government Printing Office, 2010.

______. Army Doctrine Reference Publication 6-0, *Mission Command*. Washington, DC: Government Printing Office, 2012.

______. Field Manual 3-36, *Electronic Warfare.* Washington, DC: Government Printing Office, 2012.

______. Field Manual 6-02.70, *Army Electromagnetic Spectrum Operations.* Washington, DC: Government Printing Office, 2010.

Internet Sources

Applegate, Scott. “The Principle of Maneuver in Cyber Operations.” 4th International Conference on Cyber Conflict. Academia, 2012. http://www.academia.edu/1436096/The_Principle_of_Maneuver_in_Cyber_Operations (accessed 30 June 2013).

Aucsmith, David. “A Theory of War in the Cyber Domain. Part I. An Historical Perspective.” Academia, 2012. http://www.academia.edu/1753317/A_Theory_of_War_in_the_Cyber_Domain_An_Historical_Perspective (accessed 17 May 2013).

Bachmann, Sascha-Dominik. "Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management." *Amicus Curiae* 88 (Winter 2011): 24-27. http://sas-space.sas.ac.uk/4562/1/1671-2132-1-SM.pdf (accessed 12 May 2013).

Barker, Deane. "How do you operationalize knowledge?" Gadgetopia Website. 2010. http://gadgetopia.com/post/7150 (accessed 14 October 2013).

Department of Defense. *The Department of Defense Strategy for Operating in Cyberspace.* July 2011. http://www.defense.gov/news/d20110714cyber.pdf (accessed 12 August 2013).

______. *Quadrennial Defense Review Report.* February 2010. http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf (accessed 10 May 2013).

______. Joint Publication 3-13, *Information Operations*. 2012. http://www.defenseinnovationmarketplace.mil/resources/12102012_io1.pdf (accessed 10 May 2013).

Department of Defense Dictionary. "Cyberspace." http://www.dtic.mil/doctrine/DOD_dictionary/data/c/10160.html (accessed 28 March 2013).

______. "Cyberspace Operations." http://www.dtic.mil/doctrine/DOD_dictionary/ (accessed 8 May 2013).

Freedburg, Sydney. J. "Army Electronic Warfare Goes on The Offensive: New Tech Awaits Approval." Breaking Defense Website. http://breakingdefense.com/2013/01/29/army-electronic-warfare-new-tech/ (accessed 12 June 2013).

Herbert S. Lin. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* (August 2010). http://jnslp.com/2010/08/13/offensive-cyber-operations-and-the-use-of-force/ (accessed 10 May 2013).

Infogineering. "The Differences Between Data, Information and Knowledge." http://www.infogineering.net/data-information-knowledge.htm (accessed 24 September 2013).

Joint Electronic Library. "Data Element." DOD Dictionary of Military Terms. http://www.dtic.mil/doctrine/DOD_dictionary/ (accessed 5 May 2013).

Krekel, Bryan. "US-China Economic and Security Review Commission Report on the Capability of the People's Republic of China toConduct Cyber Warfare and Computer Network Exploitation." George Washington University, 2009. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf (accessed 12 May 2013).

Leed, Maren. “Offensive Cyber Capabilities at the Operational Level.” Center for Strategic International Studies, 2013. http://csis.org/files/publication/ 130916_Leed_OffensiveCyberCapabilities_Web.pdf (accessed 12 October 2013).

Lewis, James A., and Katrina Timlin. “Cybersecurity and Cyberwarfare.” Center for Strategic and International Studies, 2011. http://www.unidir.org/files/ publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (accessed 10 May 2013).

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy* (August 2010). http://jnslp.com/2010/08/13/offensive-cyber-operations-and-the-use-of-force/ (accessed 10 May 2013).

Lipman Report Editors. “Threats to the Information Highway: Cyber Warfare, Cyber Terrorism, and Cyber Crime.” *The Guardsmark*. http://www.guardsmark.com/ files/computer_security/TLR_Oct_10.pdf (accessed 28 March 2013).

Merriam-Webster Dictionary. “Computer.” https://www.google.com/#q=definition+ of+computer (accessed 5 May 2013.)

______. “Cyber.” http://www.merriam-webster.com/dictionary/cyber (accessed 2 July 2013).

______. “Domain.” http://www.merriam-webster.com/dictionary/domain, (accessed 8 May 2013).

______. “Information Technology.” http://www.merriam-webster.com/dictionary/ information%20technology (accessed 5 May 2013).

National Museum of Computing. “The Colossus Gallery.” Codes and Cyphers Heritage Trust. http://www.tnmoc.org/explore/colossus-gallery (accessed 28 March 2013).

O’Harrow, Robert Jr., and Greg Linch. “Timeline: Key events in cyber history.” *The Washington Post*, 3 June 2012. http://www.washingtonpost.com/wp-srv/ special/investigative/zeroday/cyber-history-timeline/ (accessed 30 March 2013).

Quinn, Kristin. “Cyber Location Nexus, Closing the gap between the physical and cyber realms and what that means for GEOINT.” *Trajectory Magazine* 2 (2013). http://trajectorymagazine.com/2013-issue-2/item/1458-cyber-location-nexus.html (accessed 11 October 2013).

Rosenzweig, Paul. “Cybersecurity, An Introduction.” *Hoover Institution Journal* (2011). http://www.hoover.org/publications/defining-ideas/article/93736 (accessed 13 June 2013).

Schmitt, Michael N. “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.” *The Columbia Journal of*

Transnational Law 37 (June 1999): 885-937. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.dtic.mil%2Fcgi-bin%2FGetTRDoc%3FAD%3DADA471993&ei=43ioUsGFA-WL2AW0sYE4&usg=AFQjCNHYbIDut-cfnfvEfu_fP1AnjPsjWw&sig2=tuNKsB4oBxoaIeaxmtWIkg&bvm=bv.57799294,d.b2I (accessed 13 September 2013).

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge, NY: Cambridge University Press, 2013. http://issuu.com/nato_ccd_coe/docs/tallinnmanual/8?mode=a_p (accessed 31 March 2013).

Secretary of the United States Air Force. "Cyberspace Operations: Air Force Doctrine Document 3-12." *Cyberwar Resources Guide*. http://www.projectcyw-d.org/resources/items/show/103 (accessed 14 June 2013).

Sheldon, John. "Cyberwar." *Encyclopedia Britannica*. http://www.britannica.com/EBchecked/topic/1498241/cyberwar (accessed 10 November 2013).

United States Army Combined Arms Center. Center for Army Lessons Learned. "Fires Warfighting Function." USACAC. http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33283 (accessed 19 July 2013).

______. "Intelligence Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33288 (accessed 19 July 2013).

______. "Mission Command Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33287 (accessed 19 July 2013).

______. "Movement and Maneuver Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33285 (accessed 19 July 2013).

______. "Protection Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33286 (accessed 19 July 2013).

______. "Sustainment Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33284 (accessed 19 July 2013).

______. "Warfighting Function." http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=33276 (accessed 19 July 2013).

United Nations Interregional Crime and Justice Research Institute. "Cyberwarfare." http://www.unicri.it/special_topics/cyber_threats/cyber_crime/explanations/cyberwarfare/ (accessed 30 March 2013).

United States Joint Forces Command. *J7/J9 Pamphlet: Executive Summary of the Unified Action Handbook Series.* 2010. http://www.dtic.mil/doctrine/doctrine/jwfc/jwfcpam_uahbk.pdf (accessed 12 May 2010).

U.S. Congress. House. House Report 112-110, *Department of Defense Appropriations Bill (2011-2012).* 112th Congress. Library of Congress. http://thomas.loc.gov/cgi-bin/cpquery/?&item=&&sid=cp112p3bcL&&refer=&&r_n=hr110.112&&dbname=cp112&&sid=cp112p3bcL&&sel=TOC_173057&&sid=cp112p3bcL&r_n=hr110.112&dbname=cp112& (accessed 29 June 2013).

U.S. President. *National Security Strategy, 2010.* The White House. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 12 May 2013).

Other Sources

Clarke, Richard A. Cyber *War, The Next Threat to National Security and What to Do About It*. New York: Harper Collins, 2010.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Columbia Journal of Transnational Law*, 37 (1999): 885-937.

Witsken, Jeffrey. Interview with author, Mission Command Center of Excellent, Ft. Leavenworth, KS, 9 September 2013.